Automated Information Systems (AIS) Security Briefing

for
Permanent Employees, Part-time Employees, Students, Contractors, and Guests

To complete the application process for access to this computer asset, or to renew an existing account, the user must e-mail S/AAA@rttc.redstone.army.mil and declare that the user has read and understands the Automated Information Systems Briefing.

1. PURPOSE: The information contained in this paper should be viewed as general guidance to those of you accessing AIS at the RTTC Distributed Center. This briefing is to ensure that you are aware of your security responsibilities; recognize the vital role you play in security; and that you do not, through familiarity, become careless.

2. TYPES OF INFORMATION: In the use of AIS, you may become exposed to various levels of classified and unclassified information. Unclassified includes such as FOR OFFICIAL USE ONLY (FOUO), proprietary, and Government developed privileged information. You are hereby advised that you are, by virtue of your employment with the U.S. Government, morally and lawfully bound to protect any and all of this information or material to which you have knowledge of or access to. Those users who are not Government employees, but have been granted authorized access to our AIS, shall be responsible for their actions regardless of the security mechanisms that are in place.

3. PASSWORD PROTECTION: Your job assignment

requires receipt of a User-ID and password that permits access to AIS processing either Classified or Unclassified Sensitive information. You must bear in mind, that all passwords must be protected at the highest level of information in the system; passwords for accessing Unclassified Sensitive AIS must be protected as FOR OFFICIAL USSE ONLY (FOUO) information. You are prohibited from sharing your password with anyone.

4. CONTROLLING ACCESS: If IAS is located within your work area, you are required to monitor access to that area and be responsible for the protection of all media while within that area. Access shall be protected at the same level as the information processed on the AIS within that area. Any unauthorized access will be reported immediately to the RTTC Distributed Center ISSO. (S/AAA@rttc.redstone.army.mil)

5. COMPUTER LOGGING: Most of the computer systems you will be accessing during the performance of your duties perform logging activities, which is an administrative procedure that monitors and records the operation of our computers to prevent abuse or suspected abuse. Therefore, it is my intent to inform you that the acknowledgement of an Account Request Form for access the RTTC Distributed Center computers, also constitutes your consent and awareness of these logging records. It is also important that you know, that any time these logging records are required for official investigations, any portion of the systems logging activities under investigation any include a record of your logging activity.

6. NETWORK MONITORING: The computers you use in the performance of your duties will have internal and external network connections that allow you to exchange information. Therefore, you are put on notice that Government telecommunications systems and AIS connected to a network, are subject to periodic security testing and monitoring to ensure proper communications security (COMSEC) procedures are being observed. Use of any AIS with any network connection constitutes consent to security testing and COMSEC monitoring. Management reserves the right to monitor network use.

7. MISUSE OF GOVERNMENT PROPERTY: AIS may be used only for Government related work. You are not authorized to use any resource to create, store, and/or process games, personal letters, or any information that is not Department of Defense (DoD) business information or programs. Violators of this guidance will be subject to disciplinary action or prosecution. Management reserves the right to periodically check individual files to verify that only official authorized mission activities are performed.

8. PROTECTION INFORMATION: I am required to impress upon you the extreme need for caution and discretion in any contacts either personal or professional. As in any interesting activity, the temptation is great to refer to your professional accomplishments. You are cautioned to avoid any conversation or release of information that could result in a disclosure of Classified or Unclassified Sensitive information to unauthorized personnel.

9. PERSONAL LIABILITY FOR FRAUD AND CRIMINAL ACTIVITY IN CONNECTION WITH COMPUTERS: (Ref: Title 18, U.S. Code) Users/customers shall be aware of the following:
    - Federal law provides for punishment of up to a $250,000 fine and ten years in jail for the first offense for various offenses. Among the offenses are:
        - knowingly accesses a computer without authorization, or exceeding authorized access, and obtaining information which requires protection against unauthorized disclosures, with the intent or reason to believe that such information obtained is to be used to the injury of the U.S. or to the advantage of any foreign nation. (NOTE: The offense is for the access and not necessarily any disclosure) (10 years $250,000).
        - intentionally accesses a Government computer without authorization, and alters, damages, or destroys information or prevents authorized use of the computer;
        - accesses a Government computer without authorization, or exceeds authorized access and obtains anything of value.
    - The above prohibitions and punishments apply

to mere attempts -- even if unsuccessful -- to commit the listed crimes. Multiple accesses, or multiple attempts constitute multiple offenses for the purposes of determining punishment.

10. ADDITIONAL GUIDANCE: Further guidance, if required, may be obtained from the Information Systems Security Officer at S/AAA@rttc.redstone.army.mil, or at (256)-842-2006.

Click here for a printable version of this page.
Adobe Acrobat Reader is required.

Back to Top
Please read this Privacy & Security Notice
Last updated January 2, 2002
Please send questions or comments about this page to webmaster@rttc.army.mil